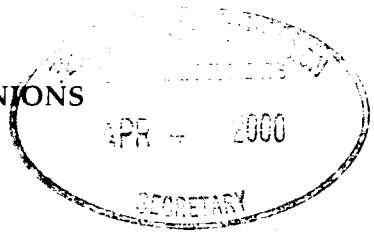
NAFCU
NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS
P.O. BOX 3769 • WASHINGTON, DC • 20007-0269
(703) 522-4770 • (800) 336-4644 • FAX (703) 524-1082



March 30, 2000

Federal Trade Commission
Secretary
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Rule, 16 CFR Part 313—Comment.

Dear Secretary:

I am writing on behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association that exclusively represents the interests of our nation's federal credit unions, in response to the interagency's request for comment on their proposed privacy regulation. In light of the fact that this rulemaking contains certain "credit union-specific" provisions and other provisions that apply to financial institutions generally, NAFCU has written under separate cover to address the "credit union-specific" portions of the NCUA's regulation. This letter will address the generally applicable portions of the interagency regulation.

§ .3 Definitions

"Collect"

Because the meaning of this term is integral in determining what types of information must be disclosed in their privacy policies, NAFCU believes that this definition should be described as clearly as possible. As proposed in the interagency rule, "collect" means to "obtain information that is organized or retrievable on a personally identifiable basis, irrespective of the source of the underlying information."[1] We urge the agencies to specify whether information that is organized or retrievable only in the aggregate is excluded from this definition. Specifically we urge the agencies to provide examples in this section indicating under what circumstances information would be considered aggregated and, therefore, non-personally identifiable[2].

[1] 65 Fed. Reg. 8,789 (2000).
[2] *See infra* discussion of personally identifiable.

"Consumer"

The proposed rule states that a person is a "consumer" if he or she obtains a financial product or service from a financial institution.[3] The examples in the regulation imply that, in order to "obtain" a product or service, the person must initiate some action with the institution, such as applying for an account or providing information to the credit union to determine qualification for a loan. Many credit unions offer trusts and custodial accounts in which a beneficiary of such account has a present or future interest in the account but no ability to utilize the services of the credit union by accessing the funds until the occurrence of some event. In these situations, the grantor, trustee or custodian may have provided certain identifying information on the beneficiary, but the beneficiary has taken no action to obtain a product or service and may have no ability to do so. Therefore, we urge the agencies to include an example in the definition of "consumer" that a beneficiary of a trust or custodial account is not a consumer until such time as the beneficiary initiates a transaction with the financial institution.

"Nonpublic Personal Information"

Due to a lack of consensus among the agencies, the proposed privacy regulations contain two alternatives for defining "nonpublic personal information." NAFCU urges the agencies, and NCUA in particular, to adopt the second alternative, "Alternative B."

Alternative B would consider information to be "publicly available" if it is lawfully attainable from a public source. Alternative A would only consider information to be "publicly available" if the financial institution *actually obtained* the information from government records, phone books or some other public database. NAFCU believes that the Alternative A reading is far too broad, therefore we do not support its inclusion in the final rule. We do, however, realize that the difference between the two approaches is, in large part, academic based on Congress' decision to include any "list, description, or other grouping of consumers . . . that is derived without using any nonpublic personal information" in the definition of nonpublic personal information.[4]

Personally Identifiable Information

NAFCU disagrees entirely with the approach that the regulators have taken to define the term "personally identifiable information." Instead of developing a working definition for this stand-alone term, the agencies have merged it into the statutory

---

[3] 65 Fed. Reg. 8,772 (2000).
[4] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

definition of "nonpublic personal information." We believe that, by giving "personally identifiable" a separate meaning, the regulation in its entirety will become far easier to understand.

> In § 509(4) of G-L-B, Congress set forth the following:
>
> (A) the term 'nonpublic personal information' means personally identifiable financial information—
> (i) provided by a consumer to a financial institution;
> (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
> (iii) otherwise obtained by the financial institution.[5]

Instead of incorporating this definition into the regulations as the definition for nonpublic personal information as Congress intended, the agencies use Congress' definition for nonpublic personal information to define "personally identifiable information." The agencies then incorporate their proposed definition for "personally identifiable" into the definition of "nonpublic personal information" by reference. NAFCU, however, believes that by taking a different approach, the agencies can provide better meaning to the term "personally identifiable" and thereby clear up some confusion that currently exists in the law.

As an initial step, NAFCU urges the agencies to look to other statutes where Congress provided a definition or explanation of what was meant by "personally identifiable:"

- Section 551 of Title 47 defines the term "personally identifiable information" as excluding any record of aggregate data which **does not identify particular persons.** (relationship between cable operators and subscribers);[6]

- 18 U.S.C. § 2710 (3) includes in the definition of the term "personally identifiable information" information which **identifies a person** as having requested or obtained specific video materials or services from a video tape service provider. (relationship between renter and video tape service provider);[7]

---

[5] *Id.*
[6] 47 U.S.C. § 551(a)(2) (emphasis added).
[7] 18 U.S.C. § 2710(3) (emphasis added).

- For purposes of protecting children's privacy on the Internet, 15 U.S.C. § 6501 defines the term "personal information" as meaning **individually identifiable** information about an individual collected online, including--
  (A) a first and last name;
  (B) a home or other physical address including street name and name of a city or town;
  (C) an e-mail address;
  (D) a telephone number;
  (E) a Social Security number;
  (F) any other identifier that the Commission determines **permits the physical or online contacting of a specific individual**; or
  (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.[8]

The common thread running throughout all three of these statutes is the correlation between identifiable information and the ability to use the covered information to distinguish one person from another. NAFCU believes that this correlation is not present in the current interagency version of the regulations.

To emphasize our point, we urge the agencies to review the Federal Trade Commission's (FTC) 1998 report to Congress addressing Internet privacy. The FTC defined personal information to include two broad categories:

> [I]nformation that can be used to identify consumers, such as name, postal or e-mail address ("personal identifying information"); and demographic and preference information (such as age, gender, income level, hobbies or interests) that can be used either in aggregate, non-identifying form for purposes such as market analysis, or in conjunction with personal identifying information to create detailed profiles of consumers.[9]

NAFCU believes that the agencies must clarify their intent – whether they mean for the regulation to include the sharing of aggregate, non-identifying information (which would seem to be at odds with Congressional intent) or whether the regulation narrowly covers information that, when shared, would allow a third party to identify a particular user of an institution's financial services. NAFCU believes that Congress only intended to cover the latter and urges the agency to adopt a similar position in the final version of the rule.

---

[8] 15 U.S.C. § 6501(8) (emphasis added).
[9] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 20 (1998).

The importance of clarification on this point is vital to the ability of financial institutions to comply with any privacy regulation. At present, the regulation is so sweeping and vaguely defined that it would appear to require that a financial institution provide privacy policies to persons that the institution has no information other than the person's name. In the context of credit unions, such a situation arises when a credit union opens a joint account for a member and a nonmember. In this instance, credit unions commonly collect "identifying" information such as address and telephone number for the member only. As a result, credit unions have no way to "collect" information on the nonmember (the limited information that the credit union does have cannot be organized or retrieved in a manner that would allow the credit union to identify the nonmember) and therefore cannot be shared with an affiliate or a nonmember third party.

The logic of NAFCU's analysis becomes obvious when a credit union or other financial institution attempts to comply with the regulation as it has been proposed. Sections .4 and .5 of the interagency rule require that initial and annual notices be sent to **all** of a financial institution's customers.[10] Section .6 indicates that these privacy statements must indicate the categories of nonpublic personal information that the institution collects. In order to "collect" information the financial institution must have obtained information about the customer and organized it in a personally identifiable manner. It is at this point that the logic of the interagency's rule falters. NAFCU believes that in order to properly analyze whether it has **collected** information about a customer, the financial institution must judge whether its information on any one customer or consumer has been aggregated (thereby making any effort to distinguish one customer from another impossible) or is **personally identifiable** allowing, as the FTC described in its report to Congress, a third party to create a detailed profile of the financial institution's customer.

Under the current rule, a financial institution never has the opportunity to determine whether it is "collecting" information about a customer or consumer. The agencies have written the regulation so broadly that financial institutions will be forced to develop and distribute privacy policies addressing how the institution protects the customer's "personally identifiable" information without taking into consideration whether the institution itself can identify the customer. NAFCU believes that, for any customer that the financial institution does not have the information necessary to physically contact that specific customer, the customer is not at risk of having his/her nonpublic information shared with a third party and is not entitled to an initial or annual notice or the right to opt-out.

---

[10] For ease of reference the term customer will be used throughout NAFCU's comment letter. It should be noted, however, that, because of the unique ownership structure of credit unions, they do not have customers they have members.

§ .4 Initial notice to consumers of privacy policies and practices required

When Initial Notice is Required

NAFCU urges the agencies to make one change to the language under proposed section .4 "Initial notice to consumers of privacy policies and practices required." As proposed, the regulation would require that financial institutions provide customers with an initial privacy statement **prior to** establishing a customer relationship. NAFCU is opposed to this timing requirement. Section 503 of G-L-B requires a financial institution to provide an initial notice **at the time of establishing** a customer relationship. NAFCU believes that the agencies' decision to amend Congress' timing requirement to require earlier disclosure can potentially add a significant burden to financial institutions.

NAFCU does not believe that Congress intended for privacy disclosures to serve a competitive function similar to the disclosures required under Regulation Z. Rather, we believe that privacy policies bring a degree of transparency to the customer in connection with the potential uses that financial institutions make of nonpublic information. We come to this conclusion based in part on Congress' reasoning for enacting Title V of G-L-B. Section 501 of G-L-B states that the policy underlying Title V is to ensure that all financial institutions have an "affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information."[11] NAFCU believes that the underlying policy of this requirement is still met if financial institutions are permitted to provide policy statements at the time of establishing a continuing relationship with a consumer.

Examples

NAFCU believes that the agencies should clarify one inconsistency in the "examples" portion of proposed § .4. Subparagraph (iii) of this section states that, "[a] bank provides the initial privacy notice to the customer so that it can be retained or obtained at a later time if the bank . . . [m]ails a printed copy of the notice to the last known address of the customer *upon request of the customer*."[12] This example, however, is inconsistent with the example given under subparagraph (i) to demonstrate when a financial institution can expect that a consumer has received actual notice. For purposes of subparagraph (i) a financial institution can expect that the consumer has received actual notice of the institution's privacy policies if the institution mails a copy of the

[11] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[12] 65 Fed. Reg. 8,799 (2000).

notice to the customer's last know address regardless of whether the customer request that it be mailed to that address.

NAFCU believes that the example under subparagraph (iii) should be modified to be consistent with the example provided under subparagraph (i). In order to accomplish this, we suggest that the agencies remove the requirement that mailing notices to the last know address be predicated on request by the customer. We are concerned that the language in subparagraph (iii) is superfluous and may cause confusion over a financial institution's ability to mail privacy policies without first obtaining authorization from its customers.

Electronic Disclosures

NAFCU supports language in the proposed rule that would allow financial institutions to post privacy policies to the Web site. We believe that this is a more practical alternative to providing notice electronically via e-mail in light of the fact that many financial institutions have incomplete records, if any, of customer's e-mail addresses.

Oral Disclosures

NAFCU has serious concerns regarding the requirement that financial institutions provide notice orally for situations where a continuing relationship is created via the telephone. Primarily, we are concerned that the legally required disclosures are so detailed and intricate that an employee will not be able to accurately inform the customer of the financial institution's privacy practices.

This concern is not inconsequential. One credit union representative informed us that the credit union adds, on average, 600 members per month via the telephone. These members are either seeking to join the credit union by purchasing at least one share of stock or by obtaining a loan through the credit union. In both cases, the credit union obtains the necessary personal information to begin the financial transaction and sends the paperwork to the member within a reasonable time to complete the transaction.

While NAFCU understands that the proposed regulations do not prohibit the credit union from following the same practice of sending written disclosures at a later point in time, we are concerned that requesting *permission* to send the privacy policy will prompt the potential member, or, for banks, customer, to request specific information regarding the policy. Although we believe that potential members are entitled to know the uses to which a credit union will put personal information, we are concerned that requesting permission to send notice at a later time will have several unintended and

deleterious consequences. First, there will be a significant cost associated with training all service representatives in connection with the nuances of the institution's privacy policy. Second, timeliness of providing services would be eroded as each representative describes the privacy policies in intricate detail.

For these reasons, we urge the agencies to permit financial institutions to provide disclosures at a later time without receiving specific permission from the customer. Such a provision will not harm the customer in light of the fact that the institution will not be collecting or sharing information regarding the customer until *after* the customer returns the necessary paperwork to finalize the transaction. We believe that, by eliminating the requirement that written notices may only be given upon permission from the customer, the agencies will ensure that financial institutions are able to carry on their day-to-day activities with the least amount of financial and staff burden, while still providing customers with the full benefit of the protection of the law.

§ .6 Information to be included in initial and annual notices of privacy policies and practices

Examples

Again, NAFCU urges the agencies to provide better consistency in their examples for what will constitute compliance. In this instance, we urge the agencies to more clearly define what they mean by a description of "categories" of information that are either collected or disclosed by the financial institution. In the example provided in subparagraph (1) of paragraph (d), the agencies indicate that a financial institution will be in compliance with the regulation if it lists the categories of information that it collects by source of information (e.g. application information, transaction information, etc.). Under subparagraph (2), however, a higher standard must be met to accurately describe the same categories of information. The only difference under subparagraph (2) is that the institution is now describing the categories of information that it discloses to affiliates or nonaffiliated third parties. In order to be in compliance with this subparagraph (2), an institution must provide an illustrative list of what would be included in the broader categories of "application" or "identifying" information. NAFCU believes that, for consistency and ease of compliance, these two sections should require that the information be described in the same manner either by broad category or representative list.

§ .13 Limitation on use of account number for marketing purposes

Language in proposed § .13 is taken directly from the statute. We believe, however, that it is necessary to provide an exception to this statutory requirement in order

to reflect practices in the marketplace that this statutory limitation was not designed to address.

On some occasions, financial institutions include an encrypted or scrambled account number somewhere in a marketing letter or response card. This is intended to permit the institution to quickly identify both the individual and that individual's account number if he/she desires to take advantage of a solicitation. The account number is never available to the nonaffiliated third party in a form that could cause the third party to have access to the account. NAFCU does not believe that Congress intended to put an end to this practice, and urges the agencies to specifically carve out an exemption indicating that account numbers may be transmitted with marketing solicitations as long as they are in a scrambled or encrypted form.

§ .15 Relation to state law

Although NAFCU understands that the preemptive language in the regulation is required by law, we believe that this issue is so important that it cannot go without comment. NAFCU fears that its members will expend tremendous resources in terms of money, staff time and system upgrades to comply with a regulation that can be preempted at the whim of a state legislature. Since our members are primarily federally chartered they often enjoy the benefit of preemption of state laws. In fact, some are so accustomed to complying **only** with federal regulations that their systems processing contracts limit internal upgrades to those required by modifications to federal regulations. In order to comply with state laws, some NAFCU members will be required to incur significant expenses outside of their existing contracts.

NAFCU supports any efforts by the agencies, other trade groups and individual financial institutions to secure a legislative amendment that will remove this preemptive language from G-L-B and the regulation.

§ .16 Effective date

Although G-L-B set an effective date of November 12, 2000, Congress also gave the agencies the authority to specify a later effective date through regulation.[13] NAFCU strongly urges the agencies to take advantage of this authority and set an effective date no sooner than six months following the statutory effective date.

Comments received by NAFCU in connection with this proposed rulemaking indicate that it could take anywhere from 6 months to 2 years for a credit union to

[13] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

ensure that its systems can handle an "opt-out." Essentially, by requiring that institutions be in compliance with the new regulation 30 days following the effective date, institutions would have to start drafting their privacy polices and updating their systems right now. This strikes NAFCU as being unfair in light of the fact that the rule is subject to change prior to its finalization. Financial institutions should not be required to expend resources and money to come into compliance with provisions that may become moot in a few short months.

Another concern for the agencies to take into consideration is cost. We encourage the agencies to adopt a rule that will allow financial institutions to include the initial notice in a mailing that the institution is already planning to make. By this we mean that if an institution only communicates with its customers once per quarter, then that institution should be allowed to send notice with its earliest planned communication with its customers.

NAFCU would like to thank you for this opportunity to share our views on the proposed privacy regulation. Should you have any questions or require additional information please call me or Gwen Baker, NAFCU's Director of Regulatory Affairs, at (703) 522-4770 or (800) 336-4644 ext. 218.

Sincerely,

Fred R. Becker, Jr.
President and CEO